

SISA



CUSTOMER — SUCCESS STORY

SISA's Transfer Impact Assessment
Strengthened Privacy and Compliance
for a Global Tech Provider.

| About the Customer

The client is a global provider of digital technology and customer experience services. Headquartered in Bengaluru, India, with operations in over 20 locations worldwide, the company delivers cutting-edge solutions in digital engineering, AI-led support, cloud, cybersecurity, and infrastructure services. Serving clients across industries like finance, telecom, and retail, the company helps organizations accelerate digital transformation and enhance customer engagement through innovation and intelligent automation

| The Business Requirement

The client required a Transfer Impact Assessment (TIA) to evaluate the privacy risks associated with the cross-border transfer of employee attendance data from the workforce management tool hosted in the US to the internal application hosted in India. This data included personally identifiable information (PII) such as employee names, IDs, working hours, leave details, overtime, and holiday records. The transfer was part of a reconciliation process conducted for client's Inc.'s US employees, initially in a UAT environment, and intended for eventual production use.

The objective was to verify whether adequate technical, organizational, and legal safeguards were in place to protect the data and ensure compliance with global privacy regulations before proceeding to production.

| The Solution

The client engaged SISA to perform a Transfer Impact Assessment (TIA) to evaluate the privacy and compliance posture of a cross-border data flow between two internal systems Workforce management tool (hosted in the United States) and internal application(hosted in India). The goal was to determine whether sufficient legal, technical, and organizational safeguards were in place to protect employee personal data during transfer.

SISA conducted the TIA through a combination of stakeholder interviews, system walkthroughs, evidence reviews, and document analysis. The assessment involved an in-depth evaluation of the following aspects:



01

Data Flow Mapping and Technical Integration Review

SISA analysed the one-way data transfer process via API between Workforce management tool and internal application. This involved validating how aggregate attendance data including PII like name, employee ID, and working hours was collected, processed, and stored in their data warehouse in India. A complete walkthrough of the data extraction logic and transfer mechanism was conducted.

02

Assessment of Legal and Contractual Safeguards

The assessment **verified the transfer mechanisms used and validated** whether appropriate contractual and organizational safeguards were in place for cross-border data transfer. The need for RoPA documentation, employee consent capture, and jurisdiction-specific compliance (India and US) were evaluated.

03

Access and Accountability Controls

The internal application access model was reviewed to determine which teams had access to extracted data. It was found that only the internal team had access; however, user accountability and disclaimers at login were missing. Recommendations were made to implement access disclaimers to ensure accountability for IT administrators and privileged users.

04

Privacy Notice and Consent Mechanism

One of the key gaps identified was the absence of a privacy notice and consent mechanism in the workforce management application during employee login. SISA recommended that a link to the privacy policy and a clear opt-in consent be implemented to enhance transparency and fulfil regulatory requirements

05

UAT Data Practices and Recommendations

During UAT, live employee data was used for testing, increasing privacy risk exposure. SISA advised replacing live PII with dummy or synthetic data in all non-production environments and avoiding any test data download to local systems.

06

Retention, Deletion, and Logging

Though retention policies existed at the enterprise level, there was no deletion log or audit trail for extracted data within the internal application database. SISA recommended implementing logging mechanisms for all API-based data extractions and deletions to support audit readiness and data lifecycle compliance.

Business Impact

The client engaged SISA to perform a Transfer Impact Assessment (TIA) to evaluate the privacy and compliance posture of a cross-border data flow between two internal systems Workforce management tool (hosted in the United States) and internal application(hosted in India). The goal was to determine whether sufficient legal, technical, and organizational safeguards were in place to protect employee personal data during transfer.

SISA conducted the TIA through a combination of stakeholder interviews, system walkthroughs, evidence reviews, and document analysis. The assessment involved an in-depth evaluation of the following aspects:

By resolving key gaps such as the absence of consent mechanisms, RoPA documentation, and audit logs the client achieved:



Improved operational transparency
in handling personal data across jurisdictions



Reduced risk exposure due to data over-retention, use of live test data, and lack of role accountability



Demonstrated accountability
through RoPA and access disclaimers, aligning with regulatory expectations



Greater stakeholder trust from U.S. counterparts, showcasing the client's proactive compliance posture

Ultimately, the TIA helped establish a robust privacy assurance framework that enables secure, lawful, and trusted data transfer practices supporting the client's business continuity and long-term reputation.

About SISA

SISA is a Global Leader in Cybersecurity Solutions for the Digital Payment Industry. As a Global Payment Forensic Investigator of the PCI Security Standards Council, we leverage forensics insights into preventive, detective, and corrective security solutions, protecting 1,000+ organizations across 40+ countries from evolving cyberthreats. Our suite of solutions from AI-driven compliance, advanced security testing, agentic detection/ response and learner focused-training has been honored with prestigious awards, including from Financial Express, DSCI-NASSCOM and The Economic Times. With commitment to innovation, and pioneering advancements in Quantum Security, Hardware Security, and Cybersecurity for AI, SISA is shaping the future of cybersecurity through cutting-edge forensics research.

Compliance	Security Testing	Cyber Defense	Data Protection & Governance	Trainings & Certifications	Leading Tech Security
Payment Data Security • PCI DSS • PCI PIN • PCI 3DS • PCI P2PE • PCI S3 • PCI S-SLC • PCI CP (Card Production) • Facilitated PCI SAQ • Quarterly Health Check-ups • Central Bank Compliance • SWIFT Strategy and Risk • CCPA • GDPR • HIPAA • ISO • NIST • SOC 1 • SOC 2 • Cloud Security • HITRUST Unified Audits Managed Compliance	Application Security • Application Penetration Testing • CREST/CERT-in Approved Security Testing • API Security Testing • Secure Code Review Network Security • Vulnerability Assessment • Penetration Testing • Configuration Review • Firewall Rule Review • PCI ASV Scan Phishing Simulation Red Teaming Exercise • Layer Security Testing	Managed Extended Detection and Response Solution - SISA ProACT • 24x7 Monitoring • UEBA • Threat Intel • Advanced Threat Hunting • Breach & Attack Simulation • SOAR • Use-case Factory Digital Forensics and Incident Response • Incident Response / Compromise Assessment Services • Forensic Readiness Audit • Forensic and Incident Response Retainer Service • PCI Forensic Investigation (PCI) • Internal Forensic Investigation (IFI) • Ransomware Simulation	Data Discovery and Classification • PCI/PII/PHI Data Discovery • Data Classification in Endpoint (Windows, Linux) • Data Classification in O365, Metadata • Dynamic Masking, Redact, Truncation • Integration to DRM, DLP, SIEM Data Privacy Professional Services • Assessments (Unified Privacy Maturity, DPIA, 3rd Party Risk) • Data Inventory, Mapping and Process flow, RoPA • Data Privacy Framework - Policy, Notice, SoPs • Consent and Notice Management framework • Data Breach and Management • Principal management • Privacy by Design implementation guide • Define Data Retention Guidelines and processes • Technical/Organization measures • Privacy Training/Awareness	Payment Data Security Training and ANAB Accredited Certification • CPISI (2 Day Program) • CPISI (3 Day Program) • CPISI- Advanced (3 Day Program) • CPISI-D (Developers) • CPISI Hybrid (4 Weeks) Certification Program in Cybersecurity for AI – CSPAI • CSPAI Forensic Briefing Sessions for Senior Management	PRISM • PRISM LLM Vulnerability Scanner Solution • AI Risk Management and Governance Solution Framework • AI Compliance and Governance Consulting Service Hardware and IoT Security Testing • Firmware Security Testing • Hardware/Embedded Security Testing • IoT Network Security Testing • IoT/Embedded Application and Management Layer Security Testing • MPOC/ PCI PTS Quantum Security • Quantum Cryptographic Consulting • Quantum Security Risk Assessment • Quantum Security Standards Compliance

SISA is a Global Leader in Cybersecurity Solutions for the Digital Payment Industry

USA | Canada | UK | Bahrain | Saudi Arabia | UAE | Qatar | India | Singapore | Malaysia | Australia

To learn more about SISA's offerings visit us at www.sisainfosec.com or

Contact your SISA sales representative at contact@sisainfosec.com

SISA

SISA

Thank You!

Follow Us:



/SISAIinfosec



/sisainfosec



/sisainfosec